Riservatezza e sicurezza delle reti

Poullet, Yves

Published in:
Internet e Privacy : Quali regole ? = Internet e Privacy : Which Rules ?, s.l., s.n.

Publication date:
1999

Document Version
le PDF de l'éditeur

Garante
per la protezione dei dati personali

«INTERNET E PRIVACY: QUALI REGOLE?»

SUPPLEMENTO N. 1
AL BOLLETTINO N. 5

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
DIPARTIMENTO PER L'INFORMAZIONE E L'EDITORIA

RISERVATEZZA E SICUREZZA DELLE RETI

Prof. Yves Poullet
Faculté Universitaire Notre-Dame de la Paix - Namur

Vorrei innanzitutto ringraziare l'amico Stefano Rodotà e tutti gli organizzatori di questo convegno, per avermi invitato in un luogo il cui prestigio è all'altezza delle sfide di cui la società deve farsi carico quando si parla dei problemi di Internet. Vi ringrazio anche per avere insistito affinché tenessi il mio intervento in francese.

Vorrei prendere in esame tre ordini di problemi. In primo luogo intendo cercare di illustrarvi quali siano i nuovi rischi connessi all'utilizzazione di Internet, i nuovi rischi per quanto riguarda la protezione dei dati. Vorrei quindi tentare un'analisi delle possibili soluzioni. Si è già parlato di PET, le Privacy Enhancing Technologies, e a tale riguardo avrei qualcosa da dire, da specificare, e vorrei anche parlare dei sistemi di autodisciplina esistenti; infine, cercherò, e questa sarà la terza parte del mio intervento, di analizzare in che modo Internet rimetta in discussione le direttive in materia di protezione dei dati.

Per quanto riguarda i nuovi rischi legati all'utilizzazione di Internet, credo sia sufficiente ricordare le quattro caratteristiche di Internet.

La prima di esse è che Internet è una rete aperta, e ciò significa che chiunque vi si può connettere e, d'altronde, che chiunque vi si può connettere per i fini più svariati - i quali non corrispondono necessariamente agli utilizzi immaginati da chi ha messo certi dati su Internet. In altre parole, è evidente che se tutto il mondo può accedervi, vi saranno problemi di segretezza in rete; se ognuno può utilizzare i dati come meglio crede, ci sarà ad esempio la possibilità, grazie ai motori di ricerca, di individuare senza problemi il profilo di personalità di un soggetto attraverso la sua presenza in un certo numero di gruppi di discussione o attraverso i siti sui quali risulta presente.

Seconda riflessione relativa al carattere aperto della rete: grazie ai legami ipertestuali, è possibile saltare da un sito Web all'altro; ciò comporta un rischio, legato al fatto che tutti i siti Web, come vedremo più avanti, sono interconnessi e possono conservare traccia del percorso effettuato su Internet. Ogni sito può sapere da dove vengo e dove sto andando, e se mi servo di determinati soggetti come fornitori di accesso, questi ultimi possono ricavare un quadro completo del tipo di utilizzo da me effettuato per quanto riguarda Internet.

La seconda caratteristica è rappresentata indubbiamente dal fatto che si tratta di una rete interattiva. Internet pone un nuovo problema, nel senso che io stesso, attraverso l'utilizzazione compiuta dal mio navigatore, genero un certo numero di dati. Sono io a generare dati personali visitando questo o quel sito. Il fatto che in un certo giorno abbia visitato un certo sito e, all'interno di tale sito, una data pagina, ad esempio la pagina sportiva del Washington Post; il fatto che da tale sito sia passato a quello di un'agenzia di viaggi, che mi sia interessato ai viaggi relativi all'Africa, ecc. ecc.; il fatto che su un sito Web abbia consultato anche le precauzioni necessarie contro l'AIDS...

Un'altra caratteristica è rappresentata senz'altro dal fatto che si tratta di una rete internazionale. Internet non conosce frontiere, e ciò significa che si possono avere paesi nei quali esistono forme di tutela, norme forti in materia di protezione, e altri paesi privi di qualsiasi regolamentazione. Risulta estremamente semplice delocalizzare un sito, e quindi a un certo momento, se un paese prevede norme eccessivamente restrittive, è facile spostare il sito in un altro paese privo di norme di sorta.

Infine, l'ultima caratteristica consiste nel fatto che Internet si caratterizza per la molteplicità degli operatori. Nel quadro di una ricerca che stiamo condu-

cendo per conto della Commissione europea, denominata E-clip, abbiamo cercato di definire una sorta di tipologia degli operatori e delle operazioni compiute, relativamente ad un'attività molto semplice quale l'acquisto di beni su Internet. E vedete, dunque, il numero dei soggetti che possono intervenire: non si tratta soltanto del venditore, ma anche del vettore o dei vettori, che possono essere numerosi, una società di ciber-marketing (ne parleremo più avanti), il fornitore di servizi Internet, la banca; vi si può aggiungere il fornitore di accesso a Internet. Ognuno di questi soggetti ha potuto raccogliere dati in una certa fase della transazione. Abbiamo elencato la tipologia dei dati volta per volta raccolti.

Ecco alcuni dei rischi connessi alle caratteristiche generali di Internet. Vorrei illustrarvi molto rapidamente come, al di là di questi rischi, ne esistano altri derivanti dal fatto che Internet non ha solo un lato visibile, ma ne ha anche uno invisibile: esiste un certo numero di trattamenti che avvengono all'insaputa dell'internauta. Si tratta in primo luogo dei trattamenti che si collocano al livello qualificabile come livello trasporto - il livello basso nell'ambito del modello ISO, ossia il modello di riferimento per quanto riguarda la standardizzazione delle reti di comunicazione.

In questo contesto non mancano i trattamenti invisibili. In primo luogo bisogna considerare che, per quanto riguarda il percorso seguito, non si deve pensare che fra due città vicine come Namur e Bruxelles (abbiamo fatto questo esperimento) il tragitto utilizzato sia quello più breve (60 Km). Il nostro messaggio in partenza da Namur transiterà per il vettore situato in Svizzera, a Ginevra, a Helsinki, a Parigi, ovvero a Washington.

Il secondo rischio è rappresentato dal fatto che, attraverso la manipolazione dei nomi di dominio (il cosiddetto «web spouting»), è possibile fare in modo che il sito Web al quale si accede non sia esattamente il sito al quale si desiderava accedere ma una sorta di sito «trompe l'oeil» - un sito cosiddetto «specchio»; recentemente un sito Web belga è stato oggetto di una perquisizione e di sanzioni penali in quanto aveva creato artificiosamente un sito che riproduceva il sito di un giornale e che evidentemente costituiva un falso ma consentiva di ottenere dati e, in particolare, dati personali.

Il comando ... è una caratteristica della rete che consente di sapere se, ad un dato momento, un altro internauta sia collegato alla rete ed utilizzi la propria connessione; è un modo indiscreto per sapere se si sta utilizzando una versione moderna del telefono.

Questo dunque per quanto riguarda i rischi invisibili legati ai livelli che si possono definire più bassi.

Per quanto riguarda i livelli più elevati, vi sono altri trattamenti non visibili, come già segnalato, vi sono altri trattamenti possibili e in particolare quelli legati all'esistenza dei cookies. Che cosa sono i cookies? Si tratta semplicemente di briciole di informazioni, ma anche di qualcosa di più, ad esempio può trattarsi di porzioni di programma che vengono inviate al vostro navigatore quando si è connessi ad un certo sito Web e che consentono a tale sito, ogniqualvolta ci si riconnetta ad esso, di riconoscere l'utente. In altri termini, se un giorno mi sono collegato al sito Web del Washington Post e il Washington Post mi ha inviato un cooky, ogni volta che mi riconnetto al Washington Post quest'ultimo potrà sapere che tre giorni, un mese o due mesi prima mi ero già collegato e quali pagine avevo specificamente consultato in quell'occasione.

Lo scopo? È chiaro che gli scopi possono essere ritenuti entro certi limiti legittimi, quando si tratti di garantire la continuità del servizio. Può avvenire che la rete Internet si interrompa, venga a cadere, e allora può essere interessante avere la possibilità di riprendere la transazione dal punto in cui essa si era fermata. Il cooky consente di farlo; il sito Web può riconoscere l'utente e quindi riprendere la transazione dal punto in cui si era interrotta.

Vi sono però scopi meno appropriati, e penso in modo particolare al marketing diretto. Il principio è il seguente: invece di avere un tipo di pubblicità da

inviare nello stesso modo a tutta la popolazione, e che non è calibrata su una persona particolare, l'interattività di Internet permette di conoscere con esattezza le preferenze dei singoli utenti e di inviare loro la pubblicità più adatta. Esistono società di ciber-marketing come Double-Click, che ha già oltre 2500 società affiliate (e si tratta di una cifra destinata verosimilmente a crescere), che raccolgono i dati di utilizzo di Internet a partire da alcuni siti che sono affiliati a tali società, dopo di che sono in grado, sulla base di questa raccolta estesa, di calibrare più precisamente le preferenze dei singoli internauti.

Se me lo consentite, vi illustro rapidamente il funzionamento di questi sistemi quando mi connetto ad un sito Web, ad esempio al sito di Altavista; è un esperimento che abbiamo compiuto più volte, e funziona molto bene - o molto male, a seconda dei punti di vista.

Quando mi connetto al sito di Altavista per effettuare una ricerca relativa ad un nome o eventualmente ad un termine, Altavista ha un legame ipertestuale (automatico) con Double-Click; ciò significa che quando mi connetto ad Altavista, la società di marketing mi invia automaticamente un cooky e riceve automaticamente un certo numero di informazioni. Si tratta in prima istanza di informazioni che comunque andrebbero inserite nell'intestazione del messaggio: la pagina che sto per visitare, il fatto che eventualmente è già stato inviato un cooky al mio navigatore, il fatto che utilizzo un certo tipo di navigatore (Netscape, e quale versione), e che lo utilizzo su un sistema operativo di una data generazione, e infine l'indirizzo dell'internauta. Quest'ultimo indirizzo non è stabile, non è fisso, e quindi si può ritenere che non si tratti di un dato personale; tuttavia, il problema riguarda le informazioni generate dal cooky, in quanto con tale cooky la società di marketing e Altavista potranno sapere non già chi sono, perché non sapremo mai chi è l'utente dietro al navigatore, bensì, e con certezza, cosa fa questo determinato utente.

Questo desideravo illustrarvi per quanto riguarda le modalità di funzionamento delle società di ciber-marketing, che a mio giudizio rappresentano un grave problema.

A conclusione di queste considerazioni sui trattamenti invisibili, vorrei aggiungere che esiste una differenza, ed una differenza netta, fra quello che l'internauta crede di fare e quello che avviene in realtà.

Che impressione si ha collegandosi a siti Web? L'impressione è che ciascuno di tali siti sia qualcosa di autonomo, che non esistano interrelazioni fra i siti. Quando ci si collega ad Altavista, sembra di uscire da Altavista e di andare in un sito 1, quindi in un sito 2, poi in un sito 3, e così via; la realtà è invece ben diversa.

Tre considerazioni si impongono a tale proposito. Primo: tutti i siti che visitiamo sono interconnessi, ossia ogni sito visitato conserva traccia del sito da noi visitato in precedenza e, ovviamente, una traccia del sito verso il quale ci spostiamo. Si tratta di un primo dato personale che può risultare interessante: tizio viene dalla pagina x, le Trois Suisses, e va alla pagina y, per esempio la Gazzetta dello Sport.

Secondo: nella misura in cui questi siti sono affiliati ad una NTTP, ad esempio una società di ciber-marketing. Perché NTTP? Ho voluto fare un piccolo gioco di parole: NTTP sta per Not-Trusted-Third-Party, ossia si tratta di un terzo non fidato che raccoglie informazioni a nostra insaputa. Bene, questo soggetto, nella misura in cui è collegato ad Altavista e al sito 1, può sapere ogni volta che tipo di utilizzazione viene compiuta del sito in questione.

Tutto ciò è lecito, e la mia impressione è che non si sia riflettuto abbastanza su questo punto: si parla molto di regolamentazione dei fornitori di accesso, si parla di regolamentare i fornitori di accesso Internet, ma non si considera con pari attenzione il fatto che chi permette tutto ciò è evidentemente il navigatore, il fatto che il navigatore consente l'invio del cooky, fa in modo che, automaticamente, per il solo fatto di utilizzare il nostro browser, siano possibili modalità di utilizzazione dei dati che mi sembrano quanto meno sleali.

Ora che abbiamo esaminato i rischi, vorrei riflettere insieme a voi su alcune soluzioni alle quali si può ricorrere per evitare tali rischi. Ma, prima di analizzare queste soluzioni, le soluzioni tecniche, autoregolamentative e legali, vorrei porvi tre domande che mi sembrano fondamentali. Per ciascuna soluzione mi sembra che ci si debbano porre tre domande.

Prima domanda: riguarda la legittimità della soluzione proposta. Legittimità nel senso di sapere se chi propone una determinata soluzione sia legittimamente autorizzato a proporla; il che non significa necessariamente che debba trattarsi di un soggetto designato in un'ottica costituzionale, ma di certo non vuol neppure dire che la legittimità implichi una discussione aperta che consenta di prendere in esame il punto di vista anche dei diretti interessati (gli internauti), e in tal senso ci si può interrogare sulla legittimità di alcune soluzioni di autoregolamentazione.

Secondo punto che mi sembra importante: il fatto che la soluzione deve essere conforme, e la conformità consiste, a mio giudizio, nella necessità che si abbia *compliance*, che si tratti di una soluzione adeguata ai principi in materia di protezione dei dati - una volta che questi ultimi siano stati definiti.

Infine, l'autoregolamentazione è un'illusione ottica se non è efficace. E per appurare se sia efficace occorre verificare se l'autorità che deve applicare l'autoregolamentazione, o eventualmente i terzi incaricati del rispetto della regolamentazione, dispongono degli strumenti necessari, se hanno la possibilità di imporre sanzioni e che tipo di sanzioni.

Fra le diverse soluzioni, la prima è quella di cui parla tutto il mondo, è senz'altro la soluzione tecnica. Mi riferisco alla definizione di Herbert: di fatto si tratta di costruzioni, di strumenti tecnici che fanno in modo che si tenti di minimizzare o di evitare del tutto che si abbiano trattamenti di dati personali.

Che cosa è già disponibile da tale punto di vista? La PET è stata definita da George Heidelberg, in un articolo che ha fatto molto rumore sull'altra riva dell'Atlantico, la *lex informatica*, che a giudizio dell'autore presentava un certo numero di vantaggi rispetto alla *lex* classica. Vanno distinti due livelli per quanto riguarda la PET. In primo luogo, un certo numero di tecniche finalizzate a consentire la protezione dei dati si collocano al livello dell'anonimato e della segretezza del messaggio. Si tratta di fare in modo che chiunque possa inviare un messaggio in modo anonimo e che tale messaggio circoli con sicurezza. La prima PET è rappresentata evidentemente dall'utilizzo di tecniche di cifratura. Vi ricordo che il Working Group di Berlino che si occupa di privacy nel settore delle telecomunicazioni aveva raccomandato fin dal 1995, quando era iniziato il dibattito relativo alla cifratura, di offrire la possibilità di utilizzare liberamente tecniche di cifratura in modo da evitare ogni rischio per la segretezza dei messaggi.

Un secondo tipo di servizi è esemplificato dalla M... finlandese, che offriva servizi di anonimizzazione - ossia servizi di corrispondenza anonima che servono esclusivamente a fare in modo che il sito web o il vostro corrispondente non possa sapere chi è il mittente del messaggio; in sostanza, chi scrive passa per un terzo, essendogli attribuito un indirizzo *just in case* - un indirizzo che permetterà ovviamente di non essere riconosciuti dalla persona cui si invia il messaggio. Si tratta di un sistema con cui si fornisce all'interessato una sorta di maschera di identità.

L'ultima possibilità è rappresentata dal cosiddetto surfing anonimo. L'idea del surfing anonimo sta prendendo sempre più piede. Durante l'ultima riunione del gruppo di Berlino sono state compiute due riflessioni. Primo punto: l'affermazione che i browser, i navigatori di Netscape, il vostro Microsoft Explorer, devono consentire la navigazione in forma anonima; sarebbe una conquista straordinaria, quella di non rivelare la propria identità. E la seconda raccomandazione che mi sembra importante riguarda la possibilità per tutti di utilizzare pseudonimi. Penso che sia un punto fondamentale quello di non dover firmare con il proprio nome, di persona identificata, bensì di poter firmare utilizzando la coper-

tura di uno pseudonimo. Sono due raccomandazioni che dovranno senz'altro trovare applicazione.

Quando si parla di PET si pensa ovviamente in primo luogo agli sviluppi più recenti, in termini di riflessione, ma anche in termini di applicazioni tecnologiche, riflessioni attuali che si riferiscono alla *piattaforma per le preferenze in tema di privacy.* L'idea è la seguente: si tratta di dare attuazione, nel settore della privacy, alle soluzioni richiamate questa mattina, le soluzioni menzionate in tema di messaggi osceni o pornografici. L'idea è di dire: utilizziamo il sistema PICS - *platform for Internet content selection* - ma utilizziamolo in modo da consentire la tutela della privacy e non soltanto la protezione nei confronti dei messaggi osceni o di altra natura.

Queste tecnologie sono state messe a punto dal Worldwide Web Consortium; come potete vedere, esso comprende interlocutori americani, francesi, giapponesi - in sostanza, tutte le società, Microsoft, Netscape, IBM, Compaq, ma anche Double-click, i grandi server, sono presenti in questo consorzio e partecipano alla sua attività.

L'idea è la seguente, la riassumo in rapporto a quattro soggetti. Il primo soggetto è l'organo di etichettatura, che deve specificare a priori il contenuto delle etichette e il loro significato. Se affermo che una società rispetta i principi di protezione dei dati, che cosa significa? In prima istanza, si tratta di sapere che cosa si intenda per dato personale. E cosa significa ciò in termini di utilizzo legittimo di tale dato? Quella certa società rispetta i principi di protezione perché utilizza i dati per sé, perché li utilizza eventualmente per esclusivi scopi di tariffazione, ovvero perché anche se li comunica, permette ai terzi di esercitare il diritto di accesso?

La prima richiesta da fare all'organo di etichettatura è la seguente : individuate una terminologia che consenta a priori di sapere che, quando si afferma che un certo sito web offre una protezione di tipo 2, bene, che si sappia cosa significa questa protezione di tipo 2 in termini di conservazione dei dati, di natura dell'utilizzo, in termini ovviamente di diritto di accesso.

In primo luogo occorre mettere a punto un vocabolario comune, e vi assicuro che è un punto estremamente delicato, estremamente difficile; la Commissione francese ha elaborato in merito una serie di riflessioni preliminari sul vocabolario utilizzato dalla P3P.

Seconda idea: fare in modo che si possa conoscere la situazione dell'etichetta. Che cosa vuol dire etichetta in materia di protezione dati? Che cosa vuol dire «etichetta 2» in materia di protezione dati? ecc. ecc. Occorre garantire la massima diffusione.

Il secondo soggetto - e si tratta ovviamente del soggetto più delicato: una volta definito il vocabolario di cui sopra, chi deve vigilare sul sito web e stabilire che un certo tipo di sito corrisponde all'etichetta di tipo 1, 2 o 3. Può trattarsi del sito web stesso, nel qual caso si parla di *self-rating*, oppure può trattarsi di un soggetto terzo, ad esempio di una società di auditing che agisca per conto del sito web.

Una volta definita l'etichetta, deve essere resa pubblica. Un certo sito web ha un'etichetta di tipo 1, 2, 3...

Cos'altro resta da fare? Resta da chiarire il ruolo di quella che può essere indicata come la società di software, e in particolare il ruolo delle società che sviluppano i programmi di navigazione. Queste ultime devono permettere, credo, due cose. In primo luogo, che il programma di navigazione sia configurato in modo da consentire all'internauta di esprimere la specifica preferenza - ossia, di dire «Per quanto mi riguarda, voglio assolutamente un livello di protezione dei dati di tipo 7, il livello più elevato».

E poi, secondo punto: una volta che abbia configurato il mio programma di navigazione con l'etichetta di tipo 7, occorre evidentemente che il mio program-

ma possa, quando incontra un sito web che non accetti un livello di protezione di tipo 7 o che offra semplicemente un livello di protezione inferiore, bene, che possa bloccare l'accesso a tale sito. Ovvero, e ciò rappresenta chiaramente un grosso progresso rispetto alla tecnologia X iniziale, ovvero che possa offrire all'internauta che si rende conto del fatto che il sito web al quale intende connettersi non possiede il livello di protezione desiderato a priori, la possibilità di dare inizio eventualmente ad un negoziato. Come dire: voi non mi garantite quella data protezione, io chiedo di avere questa protezione, che cosa mi offrite a titolo di garanzia supplementare?

Ecco quello che l'internauta, il quarto soggetto in causa, deve poter fare: se il sito web garantisce lo stesso livello di protezione, non c'è problema, si ha quello che si chiama *automatic matching*, ma se invece non viene garantito lo stesso livello, allora interviene la trattativa negoziale.

Ci sarebbero ancora molte cose da dire, ma non voglio indugiare su un punto sul quale potremo tornare più avanti - ossia, il problema della regolamentazione dei navigatori; su questo punto il nostro gruppo di ricerca ha elaborato un certo numero di raccomandazioni, che sono state presentate alla conferenza europea delle autorità di protezione dei dati. Potremo tornare su questo punto quando lo desiderate.

Per quanto riguarda l'autoregolamentazione: l'idea va vista nel contesto di un sistema di normalizzazione. Non si potrebbero definire a priori modalità di gestione di dati personali che siano conformi ai principi in materia di protezione dati. L'autodisciplina, e in questo senso è necessario distinguerla dalle PETs, pone maggiormente l'accento sulle modalità di gestione, mentre le PETs pongono evidentemente l'accento su tecnologie che, a priori, vietano l'una o l'altra modalità di gestione. Nel quadro dell'approccio ISO, il principio chiarissimo è di dire: cercheremo di definire modalità di gestione dell'informazione, all'interno delle imprese che offrono servizi via Internet, che possano essere conformi ad una serie di principi in materia di protezione dei dati.

Si tratta di un'attività cui ha dato inizio nell'ambito dell'ISO il *Consumer Policy Committee*, ma è interessante osservare la tipologia dei consumatori che si sono mostrati interessati a questo sistema e che per primi ne sono stati coinvolti.

È un sistema che ovviamente si basa su un certo numero di procedure, in quanto il problema consiste nel poter dire, una volta definito un elenco di pratiche in materia di utilizzo corretto dell'informazione, che un certo sito web si conforma allo standard definito una volta per tutte. Pertanto, il problema che si pone è come regolare la questione delle procedure di certificazione dei cittadini; come fare perché sia riconosciuta la conformità di un sito web.

Primo quesito: stiamo collaborando con società di revisione per tentare di individuare un approccio possibile. Il primo quesito sottopostoci è il seguente: la certificazione, e si tratta un po' dello stesso problema relativo alla P3P, viene compiuta dal sito web stesso, anche se deve essere effettuata necessariamente da un soggetto terzo abilitato a verificare il funzionamento dell'impresa. Si tratta di un problema di estrema delicatezza; è evidente che si avrà molta più fiducia in questa società di revisione rispetto ad un'autocertificazione, ma è chiaro d'altra parte che l'autocertificazione presenta una componente costi molto minore, mentre il processo di revisione da parte di un terzo risulta estremamente costoso.

Secondo punto importante: sapere se occorre definire standard internazionali oppure se la certificazione debba avvenire secondo standard che possono essere standard nazionali o regionali, ed ecco immediatamente il concetto: se non si possa elaborare a livello europeo uno standard, un certo numero di *fair information practices* che siano compatibili con la protezione dei dati così come prevista dalla direttiva. E, a partire da tale momento, definire il marchio europeo che potrebbe essere eventualmente un marchio di qualità entro il cosiddetto Internet globale.

Il punto successivo da chiarire è il seguente: se la certificazione sia qualcosa di volontario, se l'impresa debba essere obbligata ad attivarsi in quanto tale, ovvero se appunto sia un adempimento volontario.

Gli altri quesiti mi sembrano di facile risposta, in particolare perché non è chiaro come si possa sanzionare un sito web che, dopo essersi sottoposto ad un controllo esterno, modifichi le pratiche informazionali, e cessi quindi di essere conforme all'etichetta assegnata inizialmente.

Sempre in materia di autoregolamentazione, alcune risposte a problemi di natura maggiormente specifica. Il primo, che molti avranno incontrato e che è stato oggetto di una sentenza che ha fatto molto rumore negli USA, la famosa sentenza nel caso Heursling v. Cyber Promotion, è il problema del *junk mail*, ossia l'invio indiscriminato di corrispondenza, corrispondenza quindi indesiderata.

L'idea dell'autorità inglese di protezione dati è quella di dire: sarebbe opportuno che, al proprio indirizzo Internet, ciascuno potesse indicare che non desidera ricevere junk mail, e sarebbe opportuno che tutti i siti web o le società di promozione possano garantire il rispetto di tale indicazione inserita dallo stesso internauta.

Il secondo riguarda il problema dei motori di ricerca, come Altavista, come Lycos; si dovrebbe consentire ai singoli, ancora una volta, di far sì che, se non desiderano che il loro nome sia oggetto di una ricerca, ad esempio se io non desidero che Altavista permetta l'effettuazione di una ricerca basata sul mio nome, bene, che tali società si impegnino a non consentire ricerche in base al mio nome. Allo stesso modo, qualora si pubblichino autonomamente informazioni sul sito web, sarebbe opportuno indicare che tali informazioni non possono essere oggetto di una descrizione successiva ad una ricerca effettuata attraverso un motore di ricerca.

In terzo luogo, e si tratta di un punto di particolare interesse per quanto mi riguarda, vorrei illustravi come da un lato le direttive in materia di protezione dei dati (ne esistono due, quella generale e la direttiva sulle telecomunicazioni), come la loro interpretazione sia messa in discussione dalle prassi comunemente seguite su Internet. E vorrei inoltre illustrarvi come, se si leggono con attenzione tali direttive, si possano proporre un certo numero di requisiti ai vari soggetti che agiscono su Internet.

Parto da una prima considerazione che mi sembra veramente fondamentale. La direttiva si applica - si tratta dell'ambito specifico - esclusivamente ai dati personali: ossia, ai dati che si riferiscono ad una persona identificata o identificabile.

Dinanzi a tale definizione, Double-Click mi dice (ed ha ragione): io non tratto dati personali. Per quale motivo? Perché non so assolutamente chi vi sia dietro il navigatore di cui ho individuato il funzionamento. I dati che raccolgo sono dati di utilizzo di un navigatore X, ma non so chi vi si nasconda dietro. Esiste dunque un problema, un problema di estrema importanza: se i cookies rappresentino i dati generati dall'invio dei cookies stessi, o non piuttosto dati personali. È vero che non si sa chi si nasconda dietro ad un cooky, ma grazie al cooky è possibile sapere cosa fa questa determinata persona, pur ignorandone l'identità - il che, al limite, non riveste alcun interesse. Primo problema, e si tratta, a mio giudizio, di un problema importante in termini di interpretazione della direttiva.

Altro problema: si tratta del concetto di *processing*, di trattamento. Non posso prevedere ogni eventualità. La direttiva dà una definizione assai ampia di un concetto di trattamento, e in particolare afferma che per trattamento si intende ogni fase di utilizzo di un'operazione: ad esempio, la consultazione, l'utilizzazione, la trasmissione. ecc. . Il problema che si pone è il seguente: se mi limito a consultare un sito web, visualizzandone il contenuto sul monitor, nel qual caso non si ha alcuno scaricamento di dati in quanto li visualizzo esclusivamente sul monitor, si può parlare di trattamento ai sensi dell'articolo 2(b) della direttiva?

Non è un quesito di immediata risoluzione, in quanto in linea di principio la consultazione è sufficiente a configurare un «trattamento». Ciò significherebbe che, quando si consulta una pagina web, si è tenuti ad adempiere ad alcuni obblighi di informazione nei confronti dell'interessato e al rispetto di alcune limitazioni; in linea di principio, si sarebbe tenuti ad effettuare una notificazione presso l'autorità responsabile per la protezione dei dati, ecc., il che mi sembra un'aberrazione oltre che assai poco pratico.

Ultima definizione che mi comporta alcune difficoltà: si tratta effettivamente di un problema di fondo, relativo al concetto di consenso. È un punto importante, poiché come sapete il consenso rappresenta un fondamento di legittimità ai fini del trattamento. In ambito Internet, grazie all'interattività della rete, è possibile dare il proprio consenso ogniqualvolta si desidera accedere a un determinato sito, e acconsentire ad un determinato trattamento effettuato da tale sito. A partire da questo momento i siti web potranno sempre affermare che, nella misura in cui l'internauta abbia indicato il proprio consenso per quanto riguarda la conservazione o il tipo di utilizzo, tutto è permesso. Il consenso può divenire, nel caso di una rete interattiva, la chiave che apre tutte le porte, e a questo punto si tratta di stabilire, ad esempio, se sia legittimo che un fornitore di accesso a Internet conservi traccia di tutti gli utilizzi compiuti da uno dei propri clienti Internet.

Queste sono solo alcune delle problematiche da prendere in esame, ve ne sono molte altre. Il problema dell'applicazione della direttiva (articolo 4.1.): si afferma in modo estremamente netto che la direttiva trova applicazione qualora si utilizzino apparecchiature situate sul territorio europeo, anche per conto di un sito web situato all'estero, al di fuori del territorio dell'Unione Europea. Consideriamo il caso di un sito web situato negli USA e visitato da un cittadino europeo.

Va da sé che il sito web americano avrà bisogno di un trasferimento di dati per raccogliere dati dell'internauta, dati che sono magari necessari; in particolare, dovrà utilizzare il programma di navigazione dell'internauta europeo, che dovrà inviargli i dati eventualmente richiesti.

A questo punto si potrebbe dire, articolo 4.1(c): tutti i siti web, nella misura in cui utilizzano il programma di navigazione dell'internauta europeo, sono soggetti all'applicazione della direttiva europea. È una conclusione cui giunge un recente rapporto che rischia evidentemente di fare molto rumore, essendo destinato né più e né meno che alla Commissione europea.

Credo inoltre che sarebbe interessante esaminare l'applicazione della direttiva sulle telecomunicazioni. Farò un esempio, ma ve ne sono molti altri. Sapete che l'articolo 10 afferma che deve esistere la possibilità di opporsi al trasferimento di chiamata a terzi. La direttiva afferma tale diritto pensando al telefono: non si potrebbe immaginare che la disposizione si applichi egualmente anche ad Internet? Non si potrebbe immaginare che, per il fatto che a un dato momento, essendo collegati ad un sito web, tale sito web invii automaticamente via Interlink (l'abbiamo visto nel caso di Altavista e DoubleClick) tutti i miei dati ad un terzo, ciò risulti contrario all'articolo 17? Questo è uno dei dubbi possibili, ma ve ne sono molti altri, e vi prego di scusarmi per non avere il tempo di illustrarli tutti.

Vorrei arrivare alle conclusioni. Durante una riunione tenutasi a Bruxelles, mi trovavo seduto dinanzi ad un rappresentante americano che mi ha detto quanto segue: negli USA non abbiamo legislazione. Voi avete leggi e autorità competenti in materia di protezione dei dati - quella italiana è esemplare da tale punto di vista -, ma sono realmente efficaci? Noi, negli USA, siamo effettivamente sensibili al problema della protezione dati, e abbiamo messo a punto tecnologie efficaci. Non è che magari siamo noi americani ad avere ragione?

Penso che il mio interlocutore non avesse comunque del tutto torto, nel senso che noi europei tendiamo forse con troppa facilità a farci scudo della legislazione (o meglio, a nasconderci dietro il fatto che esiste una legislazione) e del-

l'esistenza di autorità competenti per affermare che tutto va perfettamente e che abbiamo assicurato la protezione dei dati.

Credo che si debba andare risolutamente verso una situazione in cui legislazione e tecnologia possano risultare complementari. La tecnologia non potrà evolvere in modo da tutelare i dati se non esiste una pressione legislativa di natura regolamentativa, anche al di là della pressione esercitata da parte dell'opinione pubblica. E, a tale riguardo, mancano collegamenti fra le associazioni dei consumatori e le associazioni per le libertà civili.

Per contro, la legislazione non potrà raggiungere gli obiettivi che si prefigge, e ne sono profondamente convinto, se non accetta di integrarsi con soluzioni di natura autoregolamentativa e tecnologica. In tal senso credo che il settore pubblico abbia un ruolo da svolgere, ed un ruolo dalle molteplici sfaccettature: si tratta di mettere rapidamente in atto questo ruolo per individuare risposte tecnologiche in grado di assicurare la protezione dei dati.

Terzo punto: ruolo dello Stato. Un certo numero di norme che servano da incitamento. In Belgio stiamo dibattendo sul fatto che le società che desiderano commerciare via Internet possano chiedere pagamenti anticipati solo se abbiano accettato di sottoporsi ad un controllo esterno per quanto riguarda il rispetto delle norme a tutela dei consumatori. Mi sembra un modo interessante di obbligare questi soggetti a consentire l'autoregolamentazione.

Infine, ultimo punto, e qui termino il mio intervento, il fatto che l'autorità pubblica deve svolgere un ruolo di sensibilizzazione e di educazione del pubblico, direi fin dalla scuola; tale ruolo rinvia al fatto che, in ultima analisi, la protezione dei dati spetta agli internauti stessi. Sono questi ultimi che, grazie all'interattività del sistema, potranno stabilire se accettare o meno una determinata prassi, se accettare o meno di ricevere junk mail, se opporsi o meno all'utilizzo dei propri dati per una determinata comunicazione a fini di marketing o di altra natura.

Tuttavia, quello che vorrei evitare è di ridurre il problema e la problematica della protezione da parte degli stessi internauti al concetto che tutto si basi sulla responsabilità individuale dei singoli internauti. Credo che, al di là della responsabilità individuale, esistano soluzioni nel cui ambito gli internauti devono poter chiedere collettivamente la definizione di soluzioni, anche da parte dei rispettivi organi normativi.

Stiamo lottando per le nostre libertà. Vi ringrazio per l'attenzione, e ringrazio in modo particolare gli interpreti. Grazie.